5 Keys to a Successful Identity and Access Management Implementation

DECEMBER 2009

Paul Engelbert

CA SERVICES GLOBAL SECURITY PRACTICE

ca™

Transforming
IT Management

Table of Contents

Executive Summary

Challenge

Identity and Access Management (IAM) is a core element of any sound security program. But IAM is also difficult to implement because it touches virtually every end user, numerous business processes as well as every IT application and infrastructure component. As such, successful projects require input and cooperation from many internal groups, an effort that can be difficult to organize. Perhaps even more vexing, IAM projects require a thorough understanding of the organization's current business strategy and security posture along with a clear vision of the desired security state and the steps required to get there. Too often, organizations attempt to reach that end state by implementing too much new technology at once, and fail to receive value from their efforts in a timely manner. Many organizations also fail to educate end users and IT personnel on the new technology and its impact on processes, and to perform the routine maintenance and upgrades that can deliver maximum value on their IAM project.

Opportunity

Of course many IAM implementations are successful and deliver real business results. Following these five best practices can make your IAM project one of them:

1. Know where you're going: understand where you are and where you're headed.

2. Get the right people involved: everyone from end users to IT, marketing and business executives need to play a role.

3. Implement incrementally: use a phased approach that delivers value early and often.

4. Educate, educate, educate: end users, business and IT staff alike need to be educated on the new technology and process changes.

5. The job is never done: like a new car, an IAM solution needs routine attention to stay in top form.

Benefits

Using these five best practices to guide an IAM implementation brings numerous benefits. For one, the phased approach enables you to quickly realize value from your investment, rather than waiting for many months or years. As you implement more phases, you continually add to that value. With an effective internal communications effort, you can educate end users and executives alike about the value of the project, thereby ensuring the funding you need to fully realize the strategic vision.

Ultimately, IAM serves as a business enabler to an organization by providing enhanced security, compliance with industry regulations, opportunities for new business initiatives that rely on secure access, reduced IT administration and help desk costs and improved employee productivity from features such as self-service password resets.

Identity and Access Management: A Business Imperative

Business Enabler and Compliance Requirement

An effective Identity and Access Management (IAM) solution is quickly becoming a must-have for enterprise organizations. The ability to quickly and reliably verify who is trying to access your systems, and what they are authorized to do, is both a business enabler and a core requirement for meeting regulatory demands.
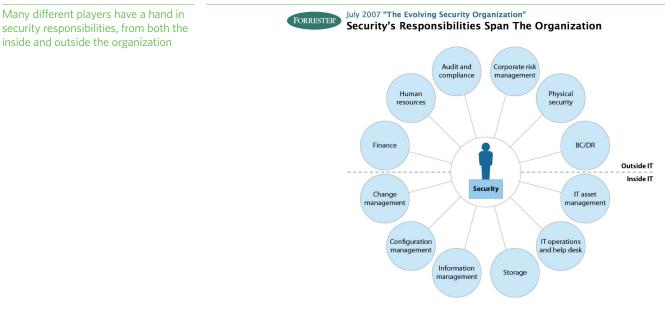
IAM enables e-commerce Web sites to provide effective customer support and more targeted sales opportunities. It is fundamental to online banking, service delivery and for retail sites that suggest products customers may want to buy based on their past purchases. IAM also enables businesses to open up portions of their network to partners, customers and suppliers, making for a more effective exchange of information that can streamline supply chains. At the same time, IAM enables new employees, contractors and business partners to more quickly get access to the applications they need to be productive and for an organization to easily stay in sync with changes to employee access rights as their roles change.

Effective identity management also helps companies comply with various government regulations, such as HIPAA privacy laws that dictate only authorized personnel see certain medical records and Sarbanes Oxley requirements for how financial information is handled.

Navigating IAM Implementation Obstacles

Too often, however, IAM implementations fall short of expectations. Security in general, and IAM in particular, is a discipline that touches virtually every individual end user and user group in the organization, as well as some fundamental IT infrastructure and business processes. As Figure A shows, many different players have a hand in security responsibilities, from both inside and outside the organization.

FIGURE A

Many different players have a hand in security responsibilities, from both the inside and outside the organization

SECURITY RESPONSIBILITIES SPAN THE ORGANIZATION

FORRESTER® July 2007 "The Evolving Security Organization"
Security's Responsibilities Span The Organization

SOURCE: "The Evolving Security Organization," Forrester Research, July 2007

Literally all users are affected by IAM, since all users of the corporate network have identities that must be managed and verified in some fashion. As such, IAM requires a thorough understanding of the existing business and security environment and a clear vision of what the desired end state looks like.

Given these challenges, it's clear that IAM projects require considerable planning and project management expertise, with a project team representing various stakeholders within the company. Most notably, like virtually any large IT project, IAM requires strong sponsorship from senior company management, who must understand the business benefits the technology can bring. And everyone involved needs to understand that, to live up to their full potential, IAM solutions require regular care and feeding long after the initial go-live date, which means planning for follow-up optimizations is crucial (see sidebar: Avoiding the IAM Pitfalls).

IAM Implementation Best Practices

With years of experience we have seen time and again what works — and what doesn't — when it comes to IAM implementations. For this paper, we have tapped the collective knowledge of these experts to come up with these five IAM implementation best practices:

KNOW WHERE YOU'RE GOING IAM is not a one-size-fits-all endeavor. You need to understand your current business and security posture, the role IAM will play in your organization and the steps you will take to get there. Most importantly, you need to have a business perspective and tie the phases of your IAM project to quantifiable business results.

GET THE RIGHT PEOPLE INVOLVED A successful IAM deployment requires cooperation among application owners, business executives and IT personnel. But you'll also need to involve marketing experts and your end users.

IMPLEMENT INCREMENTALLY Few organizations have an appetite for IT projects that go on for many months or even years before they show business value. Implementing IAM in phases can dramatically shorten the "time to value" of your project — the time before the business sees a distinct benefit — in the process giving you executive backing that will ensure the full funding of future phases.

EDUCATE, EDUCATE, EDUCATE No IT project will succeed without education of both end users and the IT staff that will be charged with ongoing administration and operation. And education is not a one-time endeavor; end users need refreshers as do IT personnel, to keep up with turnover and new product capabilities.

THE JOB IS NEVER DONE Getting full value from an IAM implementation requires that you pay regular attention to it. Like a car that needs routine maintenance, an IAM system needs maintenance to keep up with product updates, changes in the IT environment and optimizations that can continually increase the value of the solution to the organization. Additionally, there's work that may result from organizational realignments where individual departments experience altered responsibilities and/or requirements.

Figure B shows how these steps may map out to a project plan.

AN IAM PROJECT ROADMAP

SECTION 2

Know Where You're Going

To get the most out of an IAM implementation, you have to have an end goal in mind. That entails understanding your current posture, known as your "as-is" state, and coming up with a realistic plan for bridging the gap between the two. It also requires that you understand the business drivers behind the IAM initiative, to ensure IT strategy aligns with business strategy.

Take a Business Perspective

When defining your end goal, or the desired end state, be sure to do so in business terms, to show the value of the project to the organization. Instead of discussing the technical merits of a password reset capability, for example, talk instead about the productivity savings to be had. When end users forget their passwords, they can reset them online in a few seconds — and get right back to work. No more will they have to spend 15 minutes or more on the line with the help desk. That, in turn, will reduce demand on the help desk, freeing up IT personnel to work on more strategic endeavors. That's the kind of discussion that makes business executives stand up and take notice, and convinces them that you are in alignment with business goals.

Of course IAM is about a lot more than password resets. The technology also can help with resource provisioning and deprovisioning, making it a foundation for proper security, and, as noted earlier, can be an enabler for various business initiatives. The role IAM technology plays will vary greatly depending on business requirements, so you'll need to determine an IAM strategy that best fits your particular organization.

Assess your Security Maturity

Along with defining your end goal, you also need to understand the current "as-is" state of security in your company, to get a grasp on what holes need to be filled and the steps you need to take to reach that desired end state. This step requires a frank assessment of your security posture, which can be difficult for internal staff to undertake. You may want to bring in an outside service provider to conduct a readiness assessment that will provide a picture of your current infrastructure and a high-level blueprint for how you can reach the desired end state.

A major pharmaceutical company found an external services provider highly helpful in conducting a security assessment that resulted in an overarching, global IAM strategy, a revamped security and IT organization, and an integrated roadmap which ties together many existing point security solutions. The company also plans to use the assessment report for its 5-year project and budget planning.

From Vision to Roadmap

Ultimately, you want to come up with four distinct elements to your IAM project plan:

- A vision in writing for the desired end state of your IAM strategy, which is a subset of your overall security and IT strategy.

- A mission statement, backed by senior management, that defines who has what authority in making the vision a reality. It is crucial to give a sense of empowerment to the groups and individuals who are charged with implementing the IAM strategy so that everyone in the organization understands their mission — and knows that it has executive approval and support.

- A definition of success metrics, so it's clear when you've achieved your IAM goals. These definitions must be measurable and quantifiable.

- A project roadmap, which defines how you will achieve the end state, including all project phases, deliverables and a timetable. Be sure to include a discussion of process changes in the roadmap, as you will likely need to update some of your internal processes.

As you can see, it takes strategic thinking to map out an IAM project, but completing the project requires a series of tactical steps, as you'll soon see.

SECTION 3

Get the Right People Involved

IAM touches virtually everyone in an organization, so it's only natural that you need to involve representatives from your end user community as well as IT, executive management and others. Take an inclusive approach.

Executives and Business Owners

No IT project will go far without backing from business executives. You'll need their support to get funding but also to empower you to implement the solution. IAM is fundamental to the security of a company and you need one or more executive sponsors who understand that and will make it clear to all concerned that the project is important to the stewardship of the company's data and, potentially, its customers' data. The project will also affect many different areas of the business; obtaining broad buy-in will help keep the project moving when it crosses organizational boundaries.

You'll also need the active involvement of business owners to make the project successful. For example, IAM involves creating roles for different functions in the organization as well as changes to the way people do things. IT is not in the best position to define these roles or process changes; that requires the involvement of the business personnel who are closest to those areas.

Application Owners

Ultimately, an IAM solution provides access to the various applications that run your organization. It makes sense, then, to talk to the business and IT personnel who are responsible for those applications early on in the process.

The assessment and planning phase of an IAM program is a great opportunity to turn application owners into champions for an IAM initiative. Ask them about the identity management and security pain points they're experiencing. Then explain how your IAM initiative can alleviate many of their issues, such as by:

- Reducing the amount of coding they have to maintain for user authentication, authorization and auditing, because IAM essentially separates security from the application

- Providing integration so end users — be they employees, customers or business partners — can have a single user ID for all of the applications they need and enjoy single sign-on across various applications

- Alleviating the identity management burden on distributed departments and application support teams

Once they understand the direct benefits that IAM can bring, you're likely to get strong backing from business and IT staff alike, which will be crucial in helping you build the business case for the IAM solution — and getting it funded for the long term.

Marketing

IAM projects deliver benefits to virtually every group in the company. Where organizations often fall short is in effectively articulating those benefits, so the various groups understand the changes that are taking place and come to embrace them. This is essentially a marketing job and requires that you get professional help, either from your company's own marketing team or an outside firm.

A major high-end clothing retailer implemented IAM for the entire organization, including the employees in their stores who have to log in to use their cash registers. Given that many of those employees are part-time or seasonal, they would often forget their passwords, get locked out of their cash registers and have to call the help desk to get a new one. But the company did an effective job of marketing the new IAM capabilities to the employees, and to management, by explaining that they would now be able to fill out an online form and quickly get a new password. What was potentially a 20-minute debacle, often taking place with customers waiting, would become a 30-second reset. Everyone could immediately see the value in that.

Ideally, you should start marketing as soon as you have a strategy and management buy-in. Always focus your marketing efforts on the outcome, meaning what users will be able to do better and faster, as opposed to the technology underneath. And resist the temptation to let your marketing campaign get ahead of what you intend to deliver; it's better to under-promise and over-deliver.

End Users

Ultimately, it's the end users who will be most effected by an IAM system, so they should be well-represented as you scope out your project. Get involvement from users in different departments to ensure you understand how they use their various applications day to day.

That will give you a clearer picture for how they'll have to deal with the changes the IAM solution will bring.

Get Commitments

In addition to getting the right people involved, you also need to ensure they understand the time commitments that will be involved to complete the project. That goes for IT as well. The day-to-day firefighting isn't going to stop while the IAM project is underway, so you need to ensure you have certain personnel who can dedicate an appropriate amount of time to the project. In certain phases, you'll need similar commitments from the business side, such as to help with process re-engineering.

Failure to get those kinds of commitments can quickly derail a project. In one example, an Australian company appointed a single IT staffer to oversee an IAM project that was being driven largely by the IAM vendor. The vendor was on site for a week, but the IT representative consistently missed meetings, or stayed for only a short time. He ultimately took ownership of the project once it was done, but never fully understood the technology. After six months, the project had to essentially be redone.

SECTION 4

Implement Incrementally

Fully integrating an IAM solution with your existing applications, and making all the necessary process changes to fully utilize its capabilities, is a project that can take many months to complete. But that doesn't mean you have to wait until the end of the process to realize value from it. With a clear roadmap in place up front, you can implement the project in phases, first tackling tactical issues that allow you to realize value early on and incrementally adding more value as you proceed to address the bigger strategic picture. It's all about getting the business benefits out of your IT investment as soon as possible, or providing a rapid time to value. Proving the mettle of a project early on will give the business the confidence to keep investing in the project, so you can be sure future phases proceed uninterrupted.

Phase 1: Can't be Too Small

Given that IAM is technology that touches everyone in the organization, you need to make sure you get it right when you first deploy. The best way to ensure that is to start small, such as by choosing 10 interested users for a pilot. That's large enough to gather valuable feedback before you implement to a larger group. IT staff may be included as part of that group, enabling you to gather valuable technical feedback.

Be sure to keep time to value in mind by choosing to first implement a function that brings immediate, tangible benefit to the organization. The classic example is self-service password reset, which brings immediate productivity benefits for both end users and the IT department, by easing the burden on the help desk and security administrators. The goal should be to show results within 60 to 90 days.

Phase 2: Larger Rollout

Once you've gained a degree of confidence that your implementation is sound, begin a phased deployment to increasingly larger groups. Perhaps a smaller department would make sense for the next step, following by a larger one and so on.

Phase 3 and Beyond: Building on the Base

Subsequent phases will focus on adding more functionality to the deployment. A significant one is role engineering, where you define the various roles that employees play in your organization and the concomitant IT resources required for each. Accurately defining these roles is fundamental to getting value from an IAM solution because it leads the way to automated provisioning and deprovisioning of resources. When a new employee joins the organization, all you need to know is the job function the employee will fill and you'll be able to largely provision all the required resources. Ultimately, IT may not be involved in the process at all; human resources staff or department managers may be able to take all the required steps.

Act Concurrently

The process of defining the roles requires close cooperation among business and IT staff, but must be driven by the business side, since only they know the ins and outs of each role. As such, it will take time. But the process can — and should — go on concurrently with other project phases. The key is to continually finish components of the project that deliver benefits to the organization and end user, so you can realize good time to value for the project overall.

Strong project management capabilities are required to effectively plan such a phased project. Recognizing you have limited resources available, you need to be careful about overloading those resources with too many tasks to complete at the same time.

At a large IT service provider, a project manager assigned the single IAM expert the simultaneous tasks of assisting the testing team, fixing system defects, preparing end-user documentation, and preparing the production environment. Needless to say, the expert was unable to complete all of the tasks in the allocated time and the project timeline slipped. To avoid a similar fate, you need to build up IAM skills in multiple team members.

The Layered Approach

Many organizations find that tackling an IAM project in layers also makes sense, with the layers stacking up as follows:

- Implement a single enterprise user repository, with all appropriate user attributes, that can link to identities in multiple, discreet user stores tied to different applications and platforms. This is the foundation of identity management. Later, the other user repositories can gradually be decommissioned as applications are configured to use the enterprise user repository.

- Implement auditing, such that whenever you create, modify or delete an identity, a log entry gets created with details about the changes. Similarly, as users log on and access various resources, you're auditing what resources they access and the changes they make. The auditing step is fundamental to keeping in compliance with various regulations and will help with e-discovery should your organization ever be subject to a legal inquiry.

- Implement role management, as described above, with the ultimate goal being that most access rights are automatically created when you create a user ID.

That's the approach a major retailer and service provider took with an identity management project that ultimately enabled its partners to have access to its internal systems. These partners install the retailer's products in customer homes and activate service. Using IAM tools, the retailer was able to largely automate what had been a rather cumbersome process of getting new customers online. Now, partners can log in to the provider's internal billing system

to activate accounts and send test signals to newly deployed hardware at customer's homes. Customers get the products installed faster, and with less hassle, and the retailer deals with fewer phone calls from its partners while at the same time increasing partner satisfaction.

Deploy Smart

As you deploy each phase of the project, be sure to have your marketing message in sync with the rollout and your help desk staff up to speed and ready to deal with any fallout. And of course, deliver early and deliver often.

SECTION 5

Educate, Educate, Educate

Too many organizations spend significant sums of money on ambitious IT projects, only to skimp on the one facet that can really make their investments pay off: education. For IAM projects, education must extend to end users and IT staff alike, and it should not be a one-time endeavor.

IT Administrators and Operations Staff

IT personnel should be trained on their new identity management tools well before implementation begins. Only then will they be able to understand the fundamental underpinnings of the tools and concepts that will play into architectural designs. Too often, IAM projects get sidetracked when the IT staff receives training during implementation, then comes back with new ideas on how to proceed. It's much more effective to educate IT staff first and have them involved in making design decisions up front.

End Users

End users, of course, must be trained on how to use any new capabilities that will be coming their way. Keep in mind that different people learn best in different ways, so it pays to have training that's available in multiple forms, including:

- Self-instructed Web-based training, for those who are comfortable with the Web and prefer to learn at their own pace
- Instructor-led Web-based training, for those who like more explanation
- Instructor-led training with hard-copy materials, for those who prefer more formal text, with the ability to ask questions

Follow-up Training

Some form of ongoing education should be made available to everyone in the organization. Issuing gentle reminders about available options every three to six months in regular corporate communications is a realistic approach for end users.

A more formal approach is appropriate for IT personnel who bear responsibility for the IAM implementation. You need to examine how often jobs typically change in the IT group to determine an exact frequency, but every six to nine months is probably realistic. In that amount of time, you may find you have significant change in the group that is responsible for the system.

The Job is Never Done

Just as training should be recurrent, so should you plan on conducting periodic maintenance checks on your IAM implementation. Building this into the project plan will help ensure you get the full value from the solution and that you fully address your education and marketing requirements long-term.

Routine Care and Feeding

Plan on conducting a routine inspection of your IAM environment once per quarter, or at least every six to nine months, asking questions including:

- What has changed in the IT environment and how does it affect IAM? Perhaps one or more new applications have come online that significantly changes the number of logons per day the system has to process. Keeping up with such changes on a routine basis will be much easier than letting them add up over time, creating a drag on the performance of your IAM solution.

- What new IAM technologies or product versions are you ready to implement?

- Are there any new fixes or patches available?

- What can be optimized to bring added value? Optimization planning should be part of your original IAM rollout strategy.

- Are there user complaints or enhancement requests that can be addressed?

- How can processes be improved to take greater advantage of the IAM solution?

- Are you implementing your continuing education plan?

- Are you effectively marketing each new capability as you deploy it?

While the temptation may be great to congratulate one another and move on to other projects once your IAM implementation is initially up and running, you must revisit the IAM solution periodically to get full value from it. As is the case with any security related technology, the job is never really done.

Conclusion

The business benefits of IAM can be significant, but the organizations that are most likely to realize them are those that have a detailed, realistic implementation plan in place. That plan has to take into account the various groups that will need to be involved in the project and ensure that key players understand and agree to the time commitments required.

Projects that typically fail to meet expectations are those that are too ambitious. Your chances for success are far greater if you take a measured, phased approach, one that delivers a steady stream of value to the organization over time. And don't be shy about using marketing to show the value that the project is bringing. Marketing leads to project awareness, and both are key elements of success.

Like any IT project, an IAM implementation is not without its challenges. But the benefits are too great to ignore. Start small, follow these best practices and prove to yourself — and to your

executive management — the value that IAM can bring. Users and management alike will probably be pleasantly surprised with what you deliver, and asking for more.

About the Author

Paul Engelbert is Vice President of the CA Services Global Security Practice, which focuses on Identity and Access Management and Security Information Management implementations. He has more than twenty years business and security experience with an extensive background in needs analysis, architecture design, and implementation procedures. He holds a B.A. in Economics from St. Lawrence University and an M.S. in Information Systems from the University of Colorado.

CA (NASDAQ: CA), one of the world's leadiing independent,
enterprise management software companies, unifies and
simplifies complex information technology (IT) management
across the enterprise for greater business results. With our
Enterprise IT Management vision, solutions and expertise,
we help customers effectively govern, manage and secure IT.

ca™ Transforming
IT Management